GROUP KEY MANAGEMENT SCHEMES IN DISTRIBUTED COMMUNICATION ENVIRONNMENT

S.Ambika[1], S.Rajakumar[2], A.S.Anakath[3] and R.Naresh[4]

[1]Department of Computer Science and Engineering
[2]Department of Mathematics
[1,2]University College of Engineering Ariyalur,TN, India
[3]School of Compting, E.G.S.Pillay Engineering College, Nagapattinam, TN, India
[4]Department of CSE, SRM University, TN, India.

Abstract: Distributed group communication is the most optimistic approach to provide a secure group communication in many emerging network applications such as peer to peer communication, Skype, Facebook, Whatsapp, PAY-TV, Video conferencing, E-mail, Twitter and online network games. Because, in distributed group communication the data are sent from any one of the group members to the remaining group members and also there is no centralized coordinator in the distributed group communication and hence it would take more computational complexity. Moreover, in distributed group communication, the users themselves generate and distribute the necessary keys to maintain the secrecy and group membership. Hence, providing security with less computation complexity is a challenging task in distributed group communication. In this paper, a detailed survey has been done towards various distributed group communication and also comparative performance analysis has been done for all the approaches. In order to do that, we have considered various parameters such as computation complexity, communication complexity and storage complexity of both the user and the server during key generation, key distribution and key updation process. Moreover, in this paper we have also included various security challenges that need to be solved to make the distributed group communication more secure. Finally, we have also given a solution to improve the various parameters in order to increase the security and performance of the distributed communication performed in various applications.

Keywords: Distributed Group Communication, Authentication, Availability, Integrity, Non-repudiation.

1. INTRODUCTION

Today many people are participating in distributed group communication performed in variety of applications. The growth of the number of many real time network group applications results in increasing security issues and minimizing the computation complexity of the distributed group key management for a dynamic secure group communication is a challenging task. This is because, in a distributed network, each user in the network can act as a client or server of the same network to provide shared and common access to the various resources without using a key server. Moreover, in distributed network, all the tasks will be divided among the users involved in the network. Hence, it will provide effective communication and more coordination among the users efficiently.

Figure 1 shows the centralized group key management scheme where only one user act as a sponsor user/key server which maintains the information about the participating users and also manages the entire system and the remaining users acts as participating users. In this scheme, a key server alone is responsible for generate, distribute and update the keys to the participation group users. The major challenges of a centralized group key management scheme includes Scalability overhead which means the entire group communication depends on the single key server and also the operation of key updation becomes an overhead when the group size varies dynamically. And the other challenge is Storage overhead which is also not efficient because more number of keys has to be securely stored in the single key server. Moreover, if the key server fails, the entire group will be lost or affected. In addition maintaining forward and backward secrecy is very difficult when a new user joins or an existing user leaves the group.

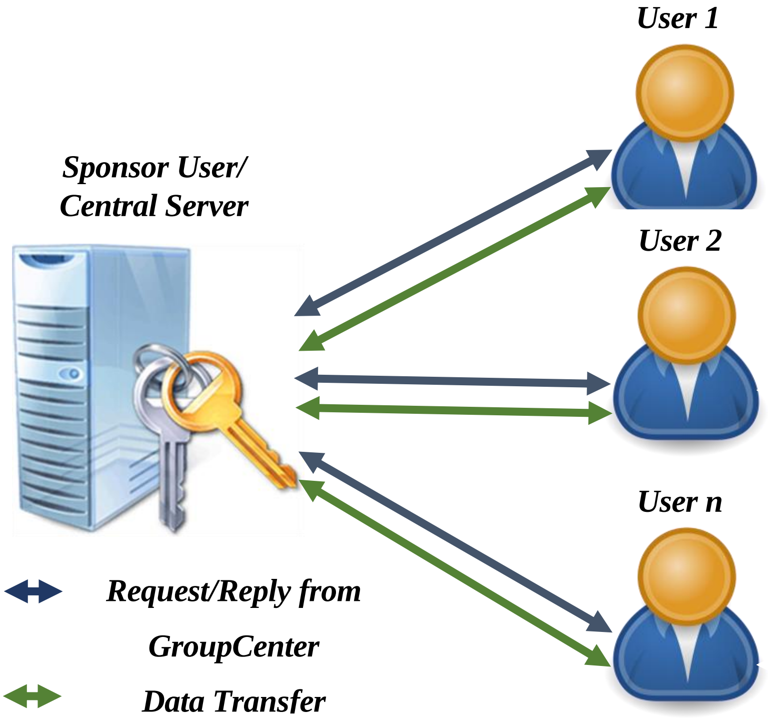

Figure 1. System model of Centralized Secure Group Communication

On contrast the the previous one, distributed group key management schemes which does not use a fixed key server, instead any user from the group can act as a key server which will be sending data to the remaining group users and where as the other users act as participating users in the group. In this scheme, any one user from the group will generating, distributing and updating the keys to the other users of the group. Each and every user of the group is able to obtain a common group key from the key received from the other existing group users.

2. DISTRIBUTED GROUP COMMUNICATION APPLICATIONS

Distributed Group Communication provides both secure and unsecure applications. Firstly, the main aim of providing the secure applications is to protect the sponsor user properties. Secondly, the goal of unsecure applications is to provide access to all public users or to even unauthorized users. Secure applications have high priority over the unsecure applications.

2.1 Unsecure Applications

These applications are also referred to as entertainment or social media comfort applications. These applications offer any users to update the information such as live updating news, photos, sharing music and movies, etc.to the group users in the network. some examples of unsecure applications are Facebook, linkedIn, open collaboration forum, twitter, etc..

2.2 Secure Applications

Secure applications utilize the subscription Pay-TV system, video conferencing, email, distributed interactive network games, e-tender quoting, e-learning, etc.. The main aim of these secure applications is to provide the information only to the authorized users or users within the group.

3. DISTRIBUTED GROUP COMMUNICATION CHARACTERISTICS

Distributed Group Communication basically provide wired or wireless communication and it has own distinct characteristics which are discussed as follows:

- **Scalability:** The group size of the distributed network remains effective when their is a significant increase or decrease in the number of users of the group which utilize the shared resources.
- **Resource Sharing:** It allows many existing authenticated users of the group to share or utilize the common resources.
- **Data Sharing:** It supports exchange of information among the group users within the dynamic group.
- **Reliability:** In a distributed network, if a failure happens for one user, the entire group will not be lost or affected because each users works independently.
- **High Performance**: In a distributed system, the group of users work together for improving the performance to complete a single task.

4. SECURITY SERVICES OF DISTRIBUTED GROUP COMMUNICATION

Security is an most important perceptive for various applications used in distributed group communication. The security services such as availability, confidentiality, integrity, authentication, non-repudiation and privacy are used to measure the various security level of distributed group communication. These security services are shown in Figure 2.

(a) Availability

Availability ensures that the entire network system is available the system ensures only to the authorized users who access resources shared by other users at any time.

(b) Confidentiality

Confidentiality conceals the transmitted information from attackers. An attacker may disclose the contents of exchanging the information by applying passive attacks. Hence, the exchanging the information should be protected when two users communicate with each other over a instant of time.

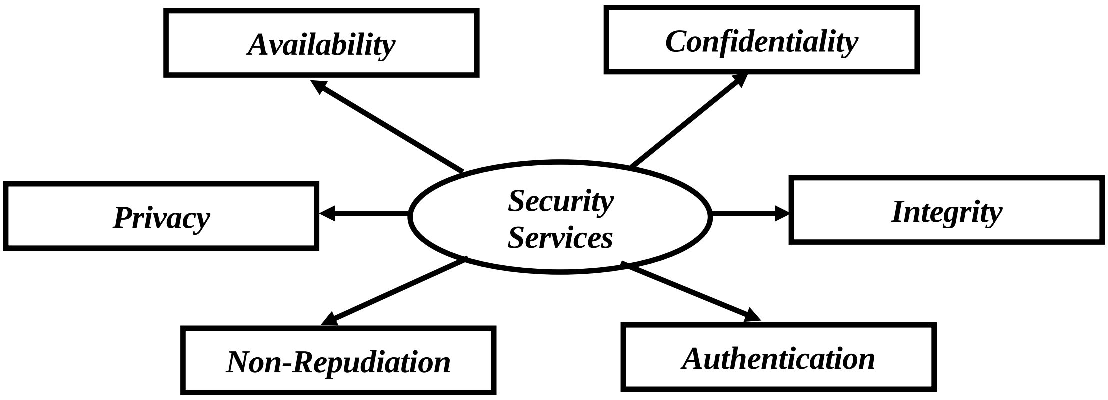

Figure. 2. Security Services

(c)Integrity

Integrity ensures that the content of the information is preserved from any alteration or modification during the transmission.

(d) Authentication

Authentication is the verification process which can be used to identify source of the message. This security service allows to accept only the messages that comes from the authenticated users.

(e)Non-repudiation

Non-repudiation is the service in which neither the sender nor the receiver can deny the transmission.

(f) Privacy

Privacy is a security service which is used for hiding the identity of a legitimate users when the data is accessed/shared during this group.

5. GROUP KEY MANAGEMENT SCHEMES

Group Key management schemes are the important component for providing the security in distributed group communication and it includes the process of generating, distributing, updating and maintaining keys which will be used to secure group communication. There are mainly two types of key management schemes available in the literature ((Bertino, 2008), (Jeong, 2008), (Xun, 2010), (Ahmad, 2012), (Younis, 2012), (v,2012)). Distributed group key management schemes are mainly divided into two types such as fully contributed group key management scheme and partially contributed group key management scheme. In the first scheme, the users themselves contribute to generate and distribute the key which helps to keep the secrecy and group management that provides security for the distributed group communication.

In a second scheme, both the users and the key server are responsible for generating and maintaining the keys and also for group management (Vijayakumar, 2016). Providing the shared access control to group communication using distributed group key management is a challenging issue. This is because of the difficulties present in handling the key generation and key distribution among the group of users where a specific number of users may join or leave the group dynamically. Therefore, in such a dynamic distributed group communication, it is necessary to allow the users to join or leave the service at any circumstances. When a new user joins the existing group to avail the service, it is the responsibility of the key server to prevent the new unauthorized user from accessing the previous information in order to provide backward secrecy in the secure group communication.

In addition, when the existing group users leave the group, they will not have any further access to the information which is available only to other users of the existing group in order to achieve the forward secrecy. Maintaining the forward secrecy and backward secrecy is also a challenging issue since the keys has to be updated for the group of users whenever a user joins or leaves the group. In this case, changing the group key takes more computation and communication complexity.

(a) Key Generation

Key Generation is the process of generating the private random keys which has to be assigned to the newly registered users and is the process of generating group keys with respect to the private keys related to the same group to provide secure distributed group communication. Here each user is generating their own secret keys from which they generate a common group key which will be performed as a public key for a group of users using distributed key management scheme.

(b) Key Distribution

Key Distribution process in secure distributed group communication is responsible for distributing the private keys and group keys to the newly registered users in a secure manner.

(c)Key Updation

In Key Updation process , any user from the group generates the group key which is based on the public key values that are received from the other group users. In this process, user of the group should take a minimum number of computations for recovering the newly generated or updated group key. Moreover, it takes minimum number of parameters for recovering the common group key at any time when the group users changes dynamically.

6. DISTRIBUTED GROUP KEY MANAGEMENT SCHEMES

In this section, a detailed survey of distributed group key management schemes has been done with respect Peer to Peer systems.

6.1 Works on Distributed Group Key Management for Peer to Peer Systems

Wallner et al. (1998) examined the challenging issues of key management for distributed group communication. It mainly concerns about the key management activities such as i) initializing the multicast group with a common group key and updating the key to the multicast group. Key updation may be necessary based on the compromise of a user. Even though, these authors obtain efficiency in terms of computation cost of key updation and storage cost, the process should be improved in order to provide better performance by avoiding communication delays in packet transmission.

Steiner et al. (2000) discussed about the new key management schemes based on the Diffie-Hellman key exchange algorithm. This scheme achieves secure and efficient key management in the perspective of dynamic user groups which are relatively small groups. Moreover this scheme supports efficient group key management only for small group communication and it is not suitable for large group communication. Wong et al (2000) proposed a new solution to the dynamic scalability problem of group or multicast group key management. They provided a new concept of key graphs for providing secure group communication. In addition, they offer three strategies for securely distributing updating key information after a user join or leave the secure group.

Wade Trappe et al. (2001) minimized the problem of access on multimedia in group communication which requires the necessity to have the key distribution and key management. They introduced a new scheme for distributing keys to use a channel independent of the multimedia information. They also proposed a second scheme, to provide multimedia in group communication which are achieved by using data-dependent channel and data embedding techniques.

Poovendran et al. (2001) discussed about the rooted-tree-based secure multicast group key distribution schemes that is helpful for collision avoidance and reduces memory requirements. Mingyan Li et al. (2002) analyzed the problem of distributing cryptographic keys to a secure distributed group communication with one sender and more than one receiver. The authors clearly discussed about the problem of deriving a key distribution model with specific group communication overhead can be posed as a constraint optimization problem. In addition, they demonstrated how to minimize the number of keys to be stored by the key server. An explicit design algorithm with the given updated key in group communication budget was also presented by them. The main advantage of their work is that they provide security for one to many group communications. But, the constraint optimization problem itself is more complex.

Wade Trappe et al. (2003) proposed the two modes of conveyance for transmitting the updated key messages which includes embedding the updating key details in multimedia information and the updated key messages linked with secure multicast group key management schemes has been hidden in the data in their approach. Moreover, this scheme utilizes minimum storage cost and the updated key messages is utilized in combination with encryption to protect the data from unauthorized users.

David et al. (2003) examines a new practical centralized hierarchical scheme for generating shared cryptographic keys for large, dynamically changing groups. This scheme is based on a bottom-up approach with the option of member contributions to the entropy of the common communications key. Unlike the previously proposed approaches that are based on information theory, One-way function algorithm provides efficient communication, computation and storage requirements that supports for dynamic large group communication.

Fei et al. (2005) developed a Video-Cassette-Recorder (VCR) based broadcast series and also proposed an active buffer management technique to provide interactive services in broadcast Video on Demand (VoD) systems. According to them, the scheme can support VCR based actions through active buffering with a high probability in a geographical range of user communication levels.

Wang et al. (2006) introduced an efficient time-bound scheme based on an algorithm called Merging. It considers only the primitive keys instead of key hierarchies which uses source coding compression. Moreover, it is possible to combine multiple keys with an aggregate key. Therefore, communication and storage costs are efficient, but the computation time is inefficient in this approach. Purandare et al. (2007) proposed a new framework for Peer to Peer (P2P) multimedia streaming, where some of the existing problems in chunk based P2P multimedia streaming is resolved using alliance based peering scheme. In this work, they offer reduction in buffering time and they achieve large dynamic group size. Xu et al. (2008) introduced a new multicast key distribution scheme which is used to reduce the computation complexity based on Maximum Distance Separable (MDS) codes to distribute multicast key dynamically. In addition, they have provided a security group communication to prevent Message-Injection Attacks.

Naranjo et al. (2010) proposed a new algorithm for group key management in which they mainly discussed about three applications to provide security and privacy. The first method is used to control the disclosure of discrete logarithm-based public keys. It can be used to secretly deliver a public key to a set of users with a minimal of only one multicast communication. The second method supports authentication technique that has been used in scenarios where the data access is provided to the authorized users alone and a public-key infrastructure is not available. The third method is based on Extended Euclidean algorithm which is a zero-knowledge proof. Moreover, it minimizes the number of messages exchanged between the two scenarios mentioned above. The main drawback of these existing works are the computation complexity involved in updating key operations are inefficient which results in poor performance.

In addition to this, the storage cost is high in most existing schemes. Bezawada et al. (2011) and vijayakumar et al. (2012) discussed about the various storage efficient key management techniques such as batch balanced, 2-3 tree, m-dimensional space geometry, merging, and rotation based key tree algorithms to support batch updating key operations. Even though the main limitations of these schemes are not suitable for the scenarios when the number of users leaves are higher than the number of users joined and Communication complexity is also high. Sun et al. (2014) proposed the binary tree method which is used for storing and managing the secret keys. In this method, each channel and group has been constructed using binary tree. The advantages of this approach are to provide flexible, scalable and dynamic group communication. The main limitation of this approach is that the dynamic group key is updated in an insecure manner and hence, it also violates backward secrecy.

Table 1. Performance of Security Services Among Existing Related Schemes

Services → **Schemes ↓**	**Forward secrecy**	**Backward secrecy**	**Privacy**	**Collusion Attack**	**Anti-eavesdrop**	**Data integrity**	**Verifiability**	**Remarks**
Wang et al. (2006)	NO	NO	NO	YES	YES	YES	YES	It takes more computation cost
Purandare et al. (2007)	YES	YES	NO	YES	YES	YES	NO	It supports large dynamic group
Xu et al. (2008)	NO	NO	YES	YES	NO	NO	NO	It prevent Message-Injection Attacks
Naranjo et al. (2010)	YES	NO	NO	YES	YES	NO	NO	It takes more storage overahead
Bezawada et al. (2011) & Vijayakumar et al. (2012)	YES	YES	NO	YES	YES	NO	NO	It takes more computation cost overahead
Sun et al. (2014)	YES	YES	YES	YES	YES	YES	YES	It violates backward secrecy
Sharma et al. (2015)	YES	YES	NO	YES	YES	YES	YES	It takes more storage overahead
Vijayakumar et al. (2016)	YES	YES	YES	NO	NO	YES	YES	It takes less computation, communication and storage overahead

Shikha Sharma et al. (2015) proposed an efficient many-to-many secure group key management scheme in distributed secure group communication. This scheme is based on Elliptic Curve Cryptography (ECC) and it utilizes minimum key size while providing securities at the same level as that of other secure system provides. This scheme mainly focuses on the issue in dynamic secure group communication and key management. A dynamic secure group communication system ensures that whenever there is a group members change, a new group key is computed and distributed to the entire group members with minimal communication and computation complexity. Moreover the advantage of this scheme is that there is no keys are getting exchanged between existing group members when the users join,or leave the group. The main drawback of the scheme is violating the forward and backward secrecy.

Vijayakumar et al. (2016) examines all these existing challenging issues in dynamic secure group communication. They introduced a novel distributed group key management protocol for secure peer to peer group communication. In this idea, a group key derivation is performed using Chinese Remainder Theorem and secure group communication is performed through the RSA encryption algorithm. The main advantage of this scheme is to minimize the computation complexity of the peer users to $O(1)$. This minimal computational complexity is achieved by performing single addition and multiplication operation when one user joins and single subtraction operation when one user leaves the operation. Hence this scheme provides a secure distributed group communication and also it maintains the forward secrecy and backward secrecy.

Table 1 summarizes the performance of the Distributed group key Management schemes discussed so far. It describes the services like forward secrecy, backward secrecy, privacy, collusion attack, anti-eavesdropping, data integrity, verifiability values which will help to improve the security of distributed group communication in Pay-TV systems.

7. CONCLUSIION

Various schemes using group key in peer to peer systems have been analysed. In a distributed circumstance, distributing cryptographic key to a variety of user group suffers with security problems. From table 1, it is obvious that various security issues arise during distributed communication. In this paper the various security shortfalls and attacks have been identified in the existing works. The drawback of each attack also exhibited. In our feature work, distributed key management for PAY TV systems, ID based key distribution in secure distributed group communication, works on Batch Rekeying and key distribution in wireless networks will be carried out.

8. REFERENCES

1. Bertino, E., Shang, N., Samuel, S. & Wagstaff Jr. (2008). An efficient time-bound hierarchical key management scheme for secure broadcasting. IEEE Transactions on Dependable and Secure Computing, 5(2), 65-70.
2. Jeong, YS., Kim, KS., Kim, YT., Park, GC., & Lee, SH. (2008). A key management protocol for securing stability of an intermediate node in wireless sensor networks. Computer and Information Technology, IEEE 8th International Conference.
3. Xun, Yi. (2010). Security of bertino-shang-wagstaff time-bound hierarchical key management scheme for secure broadcasting. IEEE Transactions on Dependable and Secure Computing, 1(99), 1489-1494.
4. Ahmad, K., Bakhache, B., Assad, SE., and Sindian, S. (2012). A scalable key management scheme for secure IP multicast over DVB-S using chaos. IEEE Mediterranean Electrotechnical Conference, France.
5. Younis, M., Farra, O., and Althouse, B. (2012). TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks", IEEE Transaction on Network and Service Management, 9(1), 100-113.
6. Kim, JY., and Choi, HK. (2012). An efficient and versatile key management protocol for secure smart grid communications, IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks, 1823-1828.
7. Vijayakumar, P., Naresh, R., Deborah, LJ., and Hafizul Islam, SK. (2016). An efficient group key agreement protocol for secure P2P communication. Security and Communication Networks, Wiley.
8. Wallner, D.M., Harder, E.J. and Agee, R.C. (1998) Key management for multicast: Issues and Architectures", Internet Draft Report, Filename: draft-wallner-key-arch-01.txt.
9. Steiner, M., Tsudik, G. and Waidner, M. (2000). Key agreement in dynamic peer groups, IEEE Transactions on Parallel and Distributed Systems, 11(8), 769-980.
10. Wong, C., Gouda, M. and Lam, S. (2000). Secure group communications using key graphs", IEEE/ACM Transactions on Networking, 8(1), 16-30.
11. Trappe, W., Song, J., Poovendran, R. and Liu, K.J.R. (2001). Key distribution for secure multimedia multicasts via data embedding. Acoustics, Speech, and Signal Processing, IEEE International Conference on, 3(1), 1449-1452.

12. Poovendran, R. and Baras, J.S. (2001). An information-theoretic approach for design and analysis of rooted-tree-based multicast key management schemes. IEEE Transactions on Information Theory, 47(1), 2824–2834.
13. Li, M., Poovendran, R. and Berenstein, C. (2002). Design of secure multicast key management schemes with communication budget constraint. IEEE Communications Letters, 6(3), 108-110.
14. Trappe, W., Song, J., Poovendran, R., and Ray Liu, K.J. (2003). Key management and distribution for secure multimedia multicast. IEEE Transactions on Multimedia, 5(4), 544-557.
15. David, A., McGrew and Sherman, A.T. (2003). Key establishment in large dynamic groups using one-way function trees. IEEE Transactions on Software Engineering, 29(5), 444-458.
16. Fei, Z., Ammar, M.H., Kamel, I. and Mukherjee, S. (2005). An active buffer management technique for providing interactive functions in broadcast video-on-demand systems. IEEE Transaction Multimedia, 7(5), 942-950.
17. Wang, W.Y. and Laih, C.S. (2006). Merging: An efficient solution for a timebound hierarchical key assignment scheme. IEEE Transactions on Dependable Secure Computing 3(1), 91–100.
18. Purandare, D., and Guha, R. (2007). An alliance based peering scheme for P2P live media streaming. IEEE Trans. Multimedia, 9(8), 1633-1644.
19. Xu, L., and Huang, C. (2008). Computation-efficient multicast key distribution. IEEE Transactions on Parallel and Distributed Systems, 19(5), 1-10.
20. Naranjo, J.A.M., Lopez-Ramosz, J.A. and Casado. L.G. (2010). Applications of the extended euclidean algorithm to privacy and secure communications, Proceedings of the 10th International Conference CMMSE.
21. Bezawada, B., Sandeep, S, and Kulkarni. (2011). Balancing revocation and storage trade-offs in secure group communication. IEEE Transactions on Dependable and Secure Computing, 8(1), 58-73.
22. Vijayakumar, P., Bose, S., and Kannan, A. (2012). Rotation based secure multicast key management for batch rekeying operations. Networking Science, Springer, 1(1), 39-47.
23. Sun, H. M., Chen, C. M., and Shieh, C. Z. (2014). Flexible-pay-per-channel: A new model for content access control in pay-TV broadcasting systems, IEEE Transactions on Multimedia, 10(6), 1109-1120.
24. Sharma, S., and Rama Krishna, C. (2015). An efficient distributed group key management using hierarchical approach with elliptic curve cryptography. IEEE International Conference on Computational Intelligence and Communication Technology.